Qui contrôle le vote électronique ?

le déclin silencieux du contrôle citoyen[1]

Ce texte ne traite que des ordinateurs de vote actuels, il ne concerne ni les ordinateurs de vote en réseau ("kiosques électroniques"), ni le vote par Internet[2].

Souligner des expressions n'indique pas leur importance, mais qu'elles renvoient vers des pages internet : la version électronique de ce document vous permet d'accéder à ces pages par simple clic.

Ce texte est susceptible d'évoluer pour répondre à des demandes d'éclaircissement ou à des informations nouvelles. ***Plutôt que de le photocopier****, imprimez sa version la plus récente depuis le site Internet, à l'adresse www.ordinateurs-de-vote.org/qui ; ce que vous avez devant les yeux date du 15 mars 2007.*

Rappel

Le vote électronique est un terme général qui englobe deux familles de systèmes :

- les **ordinateurs de vote**[3] sont placés dans les bureaux de vote. Ils enregistrent les votes et les dépouillent, sans s'occuper de l'identification de l'électeur ni de son émargement. Trois fabricants sont autorisés depuis 2004 : Nedap (néerlandais), ES&S (américain) et Indra (espagnol). Quelques dizaines de villes utilisent leurs ordinateurs, dont sept de taille moyenne : Amiens, Boulogne-Billancourt, Brest, le Havre, Reims, Le Mans, et Mulhouse. D'autres villes les ont jugés insatisfaisants : Cannes, Grenoble, Sceaux et St Denis. Plus d'un million d'électeurs sont concernés.
- le **vote par internet** s'effectue depuis n'importe quel ordinateur, par exemple à son domicile. Identification et émargement sont gérés. Contrairement aux ordinateurs de vote, il reste expérimental[4]. En France, il n'est autorisé que pour les expatriés, et seulement pour élire l'AFE (Assemblée des Français de l'Étranger), comme au mois de juin 2006.
- un intermédiaire entre les deux précédents est à l'étude : les **kiosques électroniques**. Il s'agit de terminaux placés dans les bureaux de vote, et connectés à des serveurs faisant tourner un logiciel de vote par internet. Identification et émargement sont gérés.

Qui sommes-nous ? Pour la plupart d'entre nous, des citoyens réunis par notre inquiétude face à l'arrivée des ordinateurs de vote dans nos villes respectives, sans le moindre débat[5], comme si il s'agissait de renouveler le parc de micro-ordinateurs. Je suis pour ma part informaticien, comme environ la moitié d'entre nous[6] : ce texte est donc le double point de vue d'un citoyen et d'un informaticien. Notre première réaction a été d'interroger nos mairies. Elles nous ont parlé meilleure

1 Titre inspiré par Ulrich Wiesner, informaticien allemand qui conteste en justice les dernières élections législatives réalisées avec des ordinateurs Nedap.

2 A ce sujet, nous avons publié une traduction du rapport sur SERVE, rapport qui a conduit l'armée américaine à abandonner ce projet de vote par internet. Egalement une traduction de l'audition de l'expert en sécurité informatique Bruce Schneier devant la Chambre des Représentants des États-Unis, où il explique pourquoi Internet n'est pas sécurisé, et que ce n'est pas qu'une affaire de technologie. L'élection de l'AFE de juin 2006 a donné lieu à trois rapports d'experts, tous critiques : A.Appel, B.Lang et F.Pellegrini.

3 Le terme de "machine à voter" a été introduit dans le code électoral en 1969, époque où il ne s'agissait pas d'informatique. Il n'est plus approprié aux ordinateurs actuellement utilisés.

4 En mai 2006, la CNIL a publié un état des lieux du vote par internet dans le monde.

5 Sans le moindre débat, et parfois sans même une délibération du Conseil Municipal. Ceux qui ne lisent pas les bulletins municipaux, ni la presse locale, découvrent l'existence des ordinateurs de vote au moment de l'élection.

6 Nous nous sentons obligés de le préciser régulièrement, sous peine d'être traités de passéistes, comme l'a fait le maire de Brest: « Franchement, je crois que contester la fiabilité de ces machines, c'est aussi contester à la fin du 19 ème siècle que le train pouvait être un outil performant et qu'il rendait malade ceux qui rentraient à l'intérieur. ». Passéiste est finalement un qualificatif plutôt banal : un jour, au parlement irlandais, le ministre responsable de l'introduction des ordinateurs de vote a traité d'altermondialistes les membres de l'Irish Computer Society, association professionnelle d'informaticiens.

organisation et économies, sans prendre au sérieux nos interrogations. Cela nous a incités à nous documenter sur Internet. Nous avons rapidement découvert le moratoire de fait de la Belgique[7], le refus de l'Irlande[8] d'utiliser des ordinateurs Nedap pourtant achetés massivement, l'année même où la France autorisait ce fabricant, ainsi que les innombrables difficultés des États-Unis[9]. Quelques mois après notre création, nous avons observé de près la catastrophique élection municipale du Québec[10]. Il nous est apparu que de la communauté des informaticiens avait exprimé de nombreuses réserves, comme en témoignent la prise de position de l'ACM[11], ou la "Resolution on Electronic Voting"[12], de David Dill (professeur d'informatique à Stanford). Nous avons rapidement compris l'immense potentiel des informations disponibles à l'étranger. Tout cela contrastait fortement avec l'absence d'inquiétudes en France. Nous avons par la suite interrogé les divers acteurs du vote électronique : les mairies équipées ou non, le Ministère de l'Intérieur, les organismes d'inspection (Bureau Veritas et Ceten-Apave), et les importateurs.

Qui sommes-nous ? Nous sommes aussi des porteurs de mauvaises nouvelles. Nous tenons à rappeler :

- que le vote électronique, tel que proposé, entraîne inévitablement **la disparition du contrôle citoyen des élections au profit de techniciens**[13]. Qu'il s'agit de changer de système politique : de la démocratie (le pouvoir au peuple) vers la technocratie (le pouvoir aux techniciens), en revenant à l'étymologie de ce mot. Ce changement, que l'on nous présente comme inéluctable, mérite un véritable débat national.
- qu'en pratique, ce contrôle que le citoyen est contraint de transmettre aux techniciens s'est **largement perdu en route**. La suite de ce texte vise à démontrer cela.
- que les systèmes de vote électronique actuels ont **une particularité les différenciant des autres systèmes informatiques** : l'impossibilité de contrôler leur bon fonctionnement. La cause est le secret du vote. Des comparaisons infondées sont souvent faites avec les procédures bancaires. Vous pouvez contrôler l'exactitude d'une transaction bancaire a posteriori, par

7 La Belgique a démarré les expériences de vote électronique en 1991, et cela concerne actuellement 44% des électeurs, proportion stagnant depuis 1999. Plusieurs incidents techniques: notamment Anvers et Schaerbeek (resté sans autre explication que les rayons cosmiques). Le coût est triple. Une association citoyenne combat ce système depuis 1994 ("Pour une éthique du vote automatisé" www.poureva.be), et trois des quatre partis francophones se sont maintenant prononcés contre. Un projet de loi imagine d'abandonner le vote électronique et de s'en tenir à l'automatisation du dépouillement (Nyssens 3-120).

8 L'Irlande devait voter électroniquement dès 2004 avec des ordinateurs Nedap. Suite à une contestation citoyenne croissante (que l'opposition politique n'a relayée que tout à la fin), il a été formé une commission indépendante (la CEV, "Commission on Electronic Voting") qui a conclu "être incapable de recommander" leur utilisation dans son premier rapport puis demandé d'importantes modifications dans son second rapport. 7500 ordinateurs sont donc restés dans des entrepôts, et leur abandon définitif est maintenant nettement envisagé. Cf. Irish Citizens for Trustworthy Evoting (http://evoting.cs.may.ie).

9 Les difficultés ne proviennent pas uniquement du vote électronique : les listes électorales comptent également. Le feuilleton de la présidentielle 2000 n'était pas dû au vote électronique, mais à une technologie plus ancienne : les cartes perforées. Celles-ci, mal dessinées, ont été difficiles à recompter. Au moins y avait-il quelque chose à recompter... En réaction, la législation HAVA a été votée. Elle a incité à remplacer les technologies anciennes : en 2004, environ 30% des électeurs ont utilisé des ordinateurs (semblables aux notres), et environ 30% des tabulatrices optiques (technologie inutilisée en France). La multiplication des bugs dans les ordinateurs, la prise de conscience qu'elles étaient des "boîtes noires" (noires au sens d'opaques), ainsi que la suspicion entourant la présidentielle 2004, ont popularisé le concept de bulletin papier vérifié par l'électeur . 26 des États ont incorporé ce principe à leur législation, et 13 autres y songent. Pour l'instant, les fabricants trainent les pieds pour modifier leurs ordinateurs, se contentant d'ajouter une imprimante sans réfléchir à l'ergonomie pour l'électeur, ni à la facilité de recompte. Beaucoup de législations sur le recompte sont mal adaptées. (www.VerifiedVoting.org, www.BlackBoxVoting.org, www.VotersUnite.org)

10 Le magazine Direction informatique, dans son article "Les ratés des élections municipales", a parlé de « catastrophe informatique » .

11 L'ACM (Association for Computing Machinery), association mondiale d'informaticiens fondée en 1947, comptant 80 000 membres, demande des ordinateurs de vote conçus plus rigoureusement et avec "trace d'audit vérifiée par l'électeur" (VVAT). Détails de cette résolution.

12 Signée par des universitaires, chercheurs ou experts dans le domaine de la sécurité informatique ou du vote électronique tels Andrew W. Appel, David Jefferson, Douglas W. Jones, Rebecca Mercuri, Peter Neumann, Avi Rubin, Bruce Schneier, Barbara Simons, David Wagner, Dan Wallach...

13 Lire également "L'exigence de transparence", Rapport CNIL 2003, page 93.

exemple en vérifiant vos relevés de compte, imprimés sur du papier bien tangible. Toutes les informations nécessaires à l'intégrité des données peuvent être mémorisées : il n'y a pas de secret entre vous et votre banque. Si votre réservation aérienne se perd dans l'éther informatique, on ne vous laissera pas monter dans l'avion, et vous pourrez protester, preuve de débit bancaire à l'appui. Tous les systèmes informatiques ont des conséquences vérifiables dans le monde réel. Presque tous... Si l'ordinateur modifie votre vote, qui s'en apercevra ?

- que **les ordinateurs de vote ne sont pas de «simples objets électroniques»**, comme cherche à le faire croire le marketing d'un fabricant[14], peut-être pour éviter des comparaisons désagréables avec nos micro-ordinateurs capricieux. C'est totalement fallacieux[15], et comme tous les ordinateurs, ces appareils contiennent un logiciel qui va déterminer l'essentiel de leur comportement. Connaître ce logiciel intégré est donc crucial.
- que la sécurité informatique ne se résume pas à éviter de connecter ces ordinateurs à Internet. Que la sécurité informatique, c'est compliqué, coûteux et incompréhensible par l'électeur lambda[16]. Qu'il faut **éviter de confondre fiabilité et sécurité** : un ordinateur qui ne tombe pas en panne, ne garantit pas pour autant un résultat authentique.
- que **l'accessibilité[17] par tous les électeurs n'a pas été étudiée scientifiquement** sous l'angle de l'interaction homme-machine[18]. Une enquête de satisfaction ne saurait répondre à cette question. A force de s'entendre seriner que voter sur un ordinateur, c'est très facile, quel électeur osera avouer qu'il n'est pas à l'aise ? Même en supposant que ce taux de satisfaction (ou de facilité d'utilisation) de 90 ou 95% soit réel, on se satisfait bien rapidement que 5 ou 10% des électeurs soient éloignés du vote : le vote papier obtiendrait certainement un succès au-delà de 99%.
- qu'il faut se faire à l'idée que certaines technologies puissent se révéler inapplicables. De vieux romans de science-fiction nous imaginaient tous nous déplacer dans des voitures volantes. Pourquoi cela ne s'est-il jamais réalisé ? Ce n'est pas un problème technique. Ce serait tout simplement très dangereux[19].
- que répéter mécaniquement "notre situation est différente de celle des États-Unis" élude la

14 « Nos machines n'ont rien à voir avec des ordinateurs. Ce sont de simples objets électroniques. » comme l'a déclaré à Sciences & Avenir (sept. 2006) le directeur de France-Élection (importateur de Nedap). Le journaliste a trouvé cela «difficilement défendable».
La communication municipale nous semble influencée par cette société. Quelques exemples :
« La technologie employée fait appel à des solutions mécaniques » Service élections de Brest.
« Contrairement à d'autres systèmes de vote électronique, la machine à voter ne contient pas d'éléments informatiques. » Mairie de Suresnes.
« une calculette géante plutôt qu'un ordinateur », Les nouvelles de Châtenay-Malabry, septembre 2006.

15 Cet ordinateur Nedap contient le même processeur 68000 que les Apple MacIntosh des années 80. Son logiciel intégré est constitué d'environ 25 000 lignes écrites en langage "C". Imprimer son code source nécessiterait donc des centaines de pages (cf rapport du PTB "Test report 2 - Voting machine ESI2" sur les Nedap destinés à l'Irlande, pages 6 et 7). Il faut se garder des apparences : ce sont des ordinateurs avec un boitier et un écran inhabituels. L'ES&S iVotronic est de conception semblable mais avec une interface plus moderne : un écran tactile. L'Indra est plus complexe, car il contient Windows XP.

16 Encore faudrait-il systématiquement évaluer ces ordinateurs sous l'angle de la sécurité : cela n'est jamais prévu lors de leur autorisation. D'heureux hasards font que des études de sécurité sont parfois conduites a posteriori : en Irlande, ou dans certains états des USA.
Selon les mairies, le coût est le principal frein à l'équipement. On nous annonce maintenant des ordinateurs de vote en réseau, telle e-Poll, nécessitant donc une sécurité accrue. **Où sera placé le compromis entre coût et sécurité ?**

17 L'accessibilité est la capacité à être utilisable par le maximum d'électeurs. Ne pas confondre avec la facilité d'utilisation ou l'ergonomie.

18 Une étude scientifique de l'ordinateur de vote brésilien a montré qu'il constituait une barrière à l'expression de leur vote pour une importante proportion de gens âgés, handicapés ou non familiers des ordinateurs (G.Michel-W.Cybis-M.Pimenta-J.M.Robert : "Electronic voting for all : the experience of the Brazilian computerized voting system").

19 Nous peinons déjà à réduire les accidents de la route, dus pour l'essentiel à des erreurs humaines. Imaginez des milliers de voiture se croisant dans le ciel, sans même la ressource de simplement s'arrêter sur le bord de la route en cas de problème...

question de savoir si nous suivons la même direction. Tout le monde connait le dicton “la France fait la même chose que les États-Unis avec dix ans de retard”. Tant notre organisation[20] que nos ordinateurs[21] ne sont guère différents.

- que la simplification de l'organisation matérielle des élections qu'apportent ces ordinateurs est bien réelle, mais qu'elle ne pèse pas lourd face à toutes ces questions. Il ne s'agit après tout que d'informatiser un processus rare : rien de comparable à l'automatisation du tri du courrier qui concerne des millions de lettres chaque jour. On sort un coûteux[22] ordinateur de son entrepôt environ une fois par an.

Les ordinateurs de vote sont donc bien de l'informatique. Nous ne sommes pas tous conscients de **l'infinie flexibilité de comportement d'un ordinateur**. Quand nous tournons à droite le volant d'une voiture, nous savons qu'elle se dirigera vers la droite. Il en est ainsi parce qu'il y a une liaison mécanique entre le volant et les roues.

Imaginez maintenant que l'on remplace cette liaison par un système informatique : le volant devient alors semblable à une manette de jeu, dont les capteurs sont connectés à l'entrée d'un ordinateur, et la sortie de ce dernier commande des moteurs électriques agissant sur l'orientation des roues. Sur autoroute, on peut imaginer un genre de pilote automatique : l'ordinateur ignore les signaux venant du volant, et dirige la voiture en fonction d'autres informations (cartographie de l'autoroute et position des autres véhicules). Le logiciel contenu dans cet ordinateur a toute liberté d'orienter les roues à sa guise.

En quittant l'autoroute, on débranchera ce pilote automatique. Le terme "débrancher" est trompeur : on ne coupe pas un tel système comme on éteint une lampe, sinon les roues deviendraient inertes. On se contente de basculer vers une autre partie du logiciel, dans laquelle il est censé transcrire fidèlement les gestes du conducteur.

Une conception malveillante pourrait tout aussi bien envoyer la voiture dans le décor chaque premier janvier entre minuit et quatre heures du matin. Voire se comporter ainsi seulement une fois sur dix. Définir un comportement conditionné par une date précise est l'enfance de l'art pour un programmeur informatique[23]. Pour cette raison, **simuler quelques votes peu avant l'élection, ou le matin même, n'apporte aucune garantie**[24].

Donc, qui contrôle le vote électronique ? Il est beaucoup plus aisé de répondre à la question “Qui contrôle le vote papier ?”. L'électeur peut vérifier l'essentiel par lui-même, et exercer son esprit critique, car il comprend le fonctionnement des objets en jeu (bulletin, urne...) dépourvus de technologie. Il doit seulement faire confiance à ses concitoyens assesseurs pour ne pas ouvrir l'urne avant le dépouillement, lequel est une opération publique et compréhensible par tous. Si il est méfiant, il peut demander à être assesseur. Le grand nombre de personnes impliquées dans une élection (en France : entre 200 000 et 300 000 assesseurs, plus les scrutateurs), chacune faisant une petite part du contrôle, ne permet que des fraudes sporadiques et de portée limitée.

Mais qui contrôle le vote électronique ?

- L'électeur ? Il n'a pas de preuve tangible de l'enregistrement de son vote : un ordinateur peut afficher une chose sur son écran, et en mémoriser une autre. Il n’est pas non plus assuré que son vote soit compté, faute de dépouillement dont le mécanisme soit compréhensible. Même si cet

20 Principe d'un certificateur indépendant se prononçant sur un référentiel défini par l'État. Ordinateurs protégés par le secret industriel.

21 L'iVotronic est fabriquée par ES&S, l'un des deux principaux fabricants américains. Nedap essaye de s'implanter sur le marché américain, notamment dans l'état de New-York.

22 Nedap vend ses ordinateurs environ 6000 € TTC pièce. Indra : environ 3000 €, mais il en faut plus.

23 Cette infinie flexibilité s'accompagne de la possibilité d'agir à l'avance, sans devoir être présent quand le comportement programmé se produit.

24 Il y a toutefois une utilité. Avant l'élection, le personnel municipal doit programmer l'ordinateur de vote : notamment indiquer les noms des candidats, et à quel bouton de l'ordinateur ils correspondent. "Programmer" s'entend ici dans le sens de programmer un magnétoscope, et non pas dans le sens d'écrire un logiciel. Le matin de l'élection, les assesseurs doivent s'assurer par eux-mêmes (puisqu'ils s'engagent par leur signature sur le ticket d'ouverture du scrutin) qu'il n'y ait pas d'erreur dans la programmation : deux candidats inversés, par exemple.

électeur était informaticien, il ne pourrait en savoir plus : **le code source[25] du logiciel intégré à l'ordinateur de vote est gardé secret par son fabricant**. Voudrait-il connaître dans quelles conditions cet ordinateur a été autorisé ? C'est impossible : lui communiquer le rapport de l'organisme d'inspection violerait le “secret industriel et commercial” et “pourrait compromettre le bon déroulement des élections”[26]. Ce dernier point est totalement surréaliste : l'intégrité de nos élections dépend-elle maintenant de la qualité de la serrure du placard dans lequel sont enfermés ces rapports ?

- Les assesseurs[27] ? Ils n'ont pas plus de compétences en informatique. Ils certifient l'honnêteté des élections en signant le P.V. des résultats, mais **peuvent-ils garantir autre chose que d'avoir respecté des procédures techniques** énumérées dans un mode d'emploi ?
  Par exemple, à la place d'une urne transparente dont ils vérifieraient la vacuité de leurs propres yeux, un ordinateur imprime un ticket affirmant que sa mémoire est vide. Que peuvent-ils réellement en savoir ?
  Ils surveillent physiquement l'ordinateur tout au long de la journée de l'élection, évitant ainsi que son logiciel soit modifié, mais ils n'ont aucune garantie qu'il soit authentique le matin de l'élection. Comment le pourraient-ils sinon en débutant leur journée par le désossage de l'ordinateur par un expert en sécurité informatique[28] ? Ce qui serait de toute façon transmettre leur rôle de contrôle à un tiers.
  Pire, une vérification de “checksum”[29], dont le nom même est obscur, leur donne l'**illusion d'avoir contrôlé quelque chose**. Tout en étant parfaitement inefficace puisque imprimé par le logiciel même qu'il est supposé garantir[30].
  Comment peuvent-ils certifier que l'ordinateur compte les votes exprimés par les électeurs, puisqu'ils ne peuvent surveiller les électrons d'une mémoire informatique comme ils le faisaient du contenu d'une urne : ils savaient incapable de se modifier l'encre d'un bulletin en papier placé dans une urne verrouillée.
- Les scrutateurs[31] ? Ils ne peuvent qu'assister à la magie de l'impression instantanée des résultats. Le Conseil de l'Europe recommande la "possibilité de second dépouillement"[32], mais un scrutateur peut-il obtenir autre chose que la réimpression d'un ticket ?
- Les délégués des partis ? A nouveau, leur manque de connaissances informatiques les laisse démunis. Ils devraient alors se résoudre à se faire accompagner d'un expert en sécurité informatique. Ce n'est pas le cas, probablement parce que personne n'en a compris la nécessité, et que de toute façon, rien n'est organisé techniquement pour permettre le travail de cet expert[33].
- La mairie ? Elle se fie à l'agrément donné par l'Etat aux ordinateurs de vote. Quand les ordinateurs sont achetés, comment sont-ils stockés entre deux élections ? Certainement sous clef, eu égard à

---

25 Ce qu'est le code source est expliqué en annexe de ce texte.

26 Avis de la CADA (Commission d'Accès aux Documents Administratifs) du 26 janvier 2006. Un recours devant le Conseil d'Etat est en préparation.

27 Les assesseurs sont les quatre citoyens qui entourent le président du bureau de vote. Ils doivent tous être là à l'ouverture et la clôture du scrutin, et au moins deux d'entre eux doivent être présent à tout moment de la journée. Ils proviennent de partis politiques différents. Le président est généralement un conseiller municipal.

28 Dans cet ordre d'idées, Michael Scott (Dublin City University) recommande qu'une autorité indépendante examine des ordinateurs Nedap sélectionnés aléatoirement, le soir de l'élection, dans le but de vérifier l'authenticité du logiciel intégré (rapport CEV, app. 2B, page 140).

29 Opération demandée aux assesseurs utilisant les ordinateurs Nedap/France-Élection. Le matin de l'élection, l'ordinateur imprime un ticket indiquant ces checksums : ce sont deux séries de 8 chiffres ou lettres (i.e. deux nombres 32 bits exprimés en hexadécimal). Les assesseurs vérifient qu'ils soient identiques à ce qu'indique le manuel d'utilisation. "Checksum" se traduit par "somme de contrôle" : on se demande pourquoi le terme anglais a été conservé. Pour rajouter un peu de "magie technologique" ?

30 Voir en annexe notre document détaillé : "la vérification de checksums est une duperie".

31 Les scrutateurs sont les électeurs qui participent au dépouillement, ou le surveille.

32 Recommandation Rec(2004)11 "sur les normes juridiques, opérationnelles et techniques relatives au vote électronique", point 26.

33 Le défunt projet de loi sur les ordinateurs de vote en réseau ("kiosques électroniques") allait dans cette direction : il prévoyait une "Cellule de veille technique composée des membres du bureau de vote centralisateur et d'experts désignés par le maire et les candidats." (exposé du ministère de l'Intérieur au Forum e-democratie 2005).

leur coût, mais a-t-on conscience de l'**extrême facilité de modification du logiciel intégré**[34], facilité qui n'est compensée par aucune procédure sérieuse de contrôle ? Quand les ordinateurs sont loués, la responsabilité du stockage revient au prestataire de services (en pratique, c'est la société importatrice des ordinateurs). Si une intrusion se produit dans l'entrepôt de stockage, étant donné que le but est la modification - et non pas le vol - d'un ordinateur, vérifiera-t-on l'intégrité des ordinateurs ? Sait-on même comment le faire ?

- L'Etat ?

    i. Le Ministère de l'Intérieur est à l'origine du cadre de fonctionnement de ces ordinateurs. Depuis cette impulsion initiale à leur développement, ses capacités de contrôle sont mineures : il partage avec les mairies l'organisation pratique des élections, et pour chaque modèle d'ordinateur, il délivre un agrément en se basant entièrement sur le rapport rendu par l'organisme d'inspection (Bureau Veritas ou Ceten-Apave).

    i. La DCSSI[35], habituellement en charge des questions de sécurité informatique, s'est penchée à deux reprises[36] sur les ordinateurs de vote, mais **sans rendre de rapport public**.

    ii. La CNIL (Commission nationale de l'informatique et des libertés) a fixé un cadre théorique pour le vote électronique en 2003[37], et s'est ensuite prononcée à plusieurs reprises sur les élections par Internet[38], mais jamais spécifiquement sur les ordinateurs de vote. La logique de sa mission semble de se concentrer avant tout sur les menaces envers la liberté et la vie privée, c'est à dire le respect du secret du vote. Avec les ordinateurs de vote actuels[39], l'identification et l'émargement de l'électeur se font selon les procédures traditionnelles : le secret du vote paraît[40] naturellement préservé par la séparation physique du vote et l'identification. Dans son rapport d'activité 2004[41], la CNIL recommande une “évaluation globale des dispositifs de vote électronique”, **recommandation qui n'a pas été suivie d'effet à ce jour**.

    iii. La justice : elle a été saisie par un candidat à l'élection au Barreau de Paris, concernant un vote par internet, et l'a débouté[42], au motif qu'il se “contentait d'énumérer des risques”[43]. Elle n'a

34 Ordinateurs Nedap utilisés en Irlande : deux minutes suffisent à remplacer le logiciel intégré, selon Michael Scott (Dublin City University) (rapport CEV, app. 2B, page 139). Cette facilité a été confirmée sur les ordinateurs Nedap utilisés aux Pays-Bas.
Ordinateurs Indra : le logiciel est placé sur un disque dur. Selon Ceten-Apave, organisme qui a produit le rapport pour agrément, il n'y a aucun mécanisme de signature du logiciel.
L'exigence n° 45 du Règlement technique fixant les conditions d'agrément est : “Les programmes [...] doivent être [...] stockés sous forme inaltérable.”. Les ordinateurs Nedap/France-Élection nous paraissent en violer l'esprit : leurs mémoires peuvent être considérées comme inaltérables (bien que ce soient des EPROMs, on ne peut pas les reprogrammer par le biais de l'ordinateur), mais elles sont amovibles. Les ordinateurs Indra nous semblent n'en respecter ni l'esprit ni la lettre : un disque dur permet par principe de changer facilement son contenu.

35 La DCSSI est une des cinq directions du SGDN (Secrétariat Général de la Défense Nationale), qui dépend du Premier Ministre. Elle est en charge des questions de sécurité informatique. Présentation.

36 Une première fois il y a plusieurs années, ainsi qu'à l'automne 2005. Le vote par internet a également été étudié récemment.

37 Délibération n°03-036 du 1er juillet 2003. Voir également le rapport 2003, page 92 et suivantes.

38 Français de l'Etranger (CSFE) 2003 (03-019). CCI (04-073). Barreaux de Paris (2005-272), Lyon et Nanterre.

39 Ce ne sera plus le cas avec les ordinateurs de vote en réseau du type e-Poll. Elles intègrent en un seul dispositif l'identification de l'électeur, l'enregistrement de son vote et de son émargement.

40 Mais faute de transparence, l'électeur ne peut intuitivement exclure que l'ordinateur enregistre l'ordre de passage des votants, ou encore que le boitier de contrôle des ordinateurs Nedap/France-Élection (dans les mains du président du bureau) affiche le vote que l'électeur est en train de composer. Cela amène également à réfléchir aux usages détournés de caméras miniaturisées (interdites en Italie), qui seraient moins facilement détectées dans l'environnement déjà technologique d'un bureau de vote informatisé : un câble de plus pourrait passer inaperçu (rapport CEV, app. 2B, page143). Aux Pays-Bas, il a été montré que les émissions radio-électriques des ordinateurs Nedap pouvaient trahir le choix de l'électeur. Pour cette raison, les Pays-Bas ont interdit les ordinateurs SDU lors des élections législatives de novembre 2006.

41 CNIL, rapport d'activité 2004 (paru début 2005), page 70.

42 Une première fois à Paris le 27 janvier 2005, jugement annulé par la Cour de Cassation le 7 juin 2005, et une deuxième fois à Lyon le 3 octobre 2005.

43 Il n'est pas simple d'établir une preuve informatique, à supposer que ce concept soit clairement défini. Cela implique d'avoir accès au système de vote au minimum le soir de l'élection (mais cela ne suffit pas concernant les

jamais eu à se prononcer sur une élection politique effectuée sur des ordinateurs de vote.

- L'organisme d'inspection (Bureau Veritas ou Ceten-Apave) ? Il examine un ordinateur à un moment donné : **l'agrément est accordé sur un modèle d'ordinateur, et non pas pour chaque exemplaire fabriqué de cet ordinateur.** Il n'accède parfois pas au code source de son logiciel : la CNIL le recommande[44], mais le “Règlement technique” ne l'impose pas. Il n'est pas clair si ce logiciel peut évoluer par la suite sans nécessiter une nouvelle procédure d'agrément[45]. On ne demande pas à cet organisme d'évaluer globalement la sécurité, mais seulement de vérifier la conformité à **un cahier des charges[46] qui a ses limites**. Ce dernier répond avant tout aux besoins des municipalités : fiabilité de l'électronique, longévité et facilité d'utilisation. En résumé, on pose à ces organismes une question très précise : comme cette question (le “Règlement technique”) est mal posée, la réponse (le rapport rendu) ne présente guère d'intérêt[47].
- A l'extrémité de la chaine, se situent le fabricant et son importateur[48]. Une organisation bien conçue devrait avoir pour but d'éviter de se poser des questions à leur sujet. **Le contrôle devrait être exercé par les premiers maillons de la chaine : en démocratie représentative, les seuls légitimes sont les électeurs, les assesseurs, les délégués et les scrutateurs.** Ce dernier maillon est en effet hautement critique. Nul besoin d'imaginer la collusion de toute une entreprise avec un parti politique. Un petit nombre (peut-être même un seul) de programmeurs ou de techniciens de la chaîne de fabrication peuvent, d'une action unique, compromettre des centaines d'ordinateurs, et donc une élection entière. Ce cas de figure est celui permettant la fraude la plus efficace. Il illustre une règle générale de l'informatique : c**elle-ci permet de faire ce qui était auparavant manuel, à plus grande échelle, parfois longtemps à l'avance, sans se déplacer, sans laisser de traces[49] et avec moins de personnel (parfois tout seul)[50]**. D'autre part, le modèle économique de ces entreprises est la cause du secret qui entoure les ordinateurs de vote[51].

A quelle conclusion cela nous amène-t-il ?

Elle pourrait s'articuler autour des mots suivants : **le contrôle (que l'on appelle aussi vérifiabilité) et la transparence. Ils manquent tous les deux cruellement.** La confiance, pour être fondée, doit s'appuyer sur son corollaire : le contrôle. Pour que cette confiance ne soit pas aveugle, la transparence doit être totale.

Quelle solution préconisons-nous ?

J'entends déjà certains se demander cela. Soyons clairs : nous n'avons pas créé le problème, nous avons déjà bien du mal à alerter à son sujet, alors nous ne nous sentons pas tenus d'apporter une solution. **La charge de la preuve ne devrait pas nous incomber**. Aux promoteurs du vote

---

manipulations qui effacent leurs traces une fois leur forfait accompli, ou qui n'en laissent pas de significatives). Cet accès n'est pas facilité par le secret industriel ajouté aux légitimes exigences de sécurité entourant le scrutin.

44 « La Commission estime que dans le cas d'une élection organisée par une collectivité publique, **le code source des logiciels utilisés par le système de vote électronique devrait être accessible sans restriction**, afin de permettre la réalisation de toutes les expertises jugées nécessaires. », délibération 03-036 du 1er juillet 2003.

45 Par exemple, aux Etats-Unis, la NASED indique quel numéro de version du logiciel intégré de l'ES&S iVotronic est certifié. Rien n'apparait dans l'arrêté d'agrément français. Le paragraphe 2.2.1 du “règlement technique”, concernant les "modifications à l'initiative du fabricant" ne dit rien sur le logiciel.

46 C'est à dire toujours ce même “règlement technique fixant les conditions d'agrément des machines à voter”.

47 Notre interlocuteur chez l'un des organismes concernés nous a confié qu'il aurait apprécié que son entreprise ait pu jouer un rôle dans la rédaction du “règlement technique”. Chez un autre organisme, il espérait que le “règlement technique” soit amélioré d'ici les élections de 2007.

48 France-Élection importe Nedap des Pays-Bas, Datamatique importe ES&S des États-Unis, Berger-Levrault importe Indra d'Espagne.

49 Ou alors des traces sans valeur juridique, ou plus simplement un résultat électoral plausible n'incitera pas à faire l'effort de les rechercher.

50 Le Pr Roberto Di Cosmo, auteur de l'article "E-duquons l'e-citoyen !", emploie l'analogie suivante : votre facteur ouvre peut-être votre courrier à la vapeur, pour le lire à votre insu. Ce serait désagréable, mais ce ne serait que quelques lettres à un endroit précis. L'équivalent électronique serait un ordinateur qui analyse vos courriels. Lui donner à examiner les courriels de tout le monde n'aurait rien d'irréaliste...

51 La sécurité est un prétexte : il s'agit du concept discutable de "sécurité par l'obscurité" (cf note n°55). La véritable raison est que l'investissement fait par ces sociétés est en grande part le développement du logiciel intégré.

électronique de démontrer son innocuité. Le **principe de précaution** doit s'appliquer également dans ce domaine. Toutefois, quelques pistes existent.

Concernant le manque de contrôle, la solution généralement préconisée[52] par les universitaires et les spécialistes en sécurité informatique, est la mise en oeuvre d'une **"trace d'audit vérifiée par l'électeur" (VVAT)**[53], c'est à dire que les ordinateurs conservent une trace physique inaltérable de l'intention de l'électeur, trace ensuite comptée indépendamment de l'informatique. En l'étant actuel de la science, cette "trace d'audit" n'est réalisable qu'avec du papier.

Concernant le manque de transparence, la solution réside dans des systèmes de conception totalement ouverte, tant au niveau matériel que logiciel. Comme les clients des systèmes de vote sont des collectivités publiques, le modèle du Logiciel Libre est ici particulièrement pertinent[54]. La sécurité, actuellement basée sur le concept douteux de "sécurité par l'obscurité"[55], en serait renforcée. **Il faut toutefois garder à l'esprit qu'obtenir la transparence sans garantir le contrôle est quasiment inutile.** Le code source d'un logiciel a beau être publié sur Internet, si vous ne pouvez garantir que ce même logiciel est présent dans tous les ordinateurs le jour de l'élection, vous n'avez guère progressé.

Notre système politique est la démocratie représentative. La plupart d'entre nous ne participent pas aux décisions politiques. Néanmoins **détenteurs de la "souveraineté populaire"**, nous déléguons temporairement notre pouvoir à nos maires, à nos députés, à notre président... pour cinq ou six années. Nous ne détenons réellement le pouvoir que le jour des élections. Durant ce jour précis, pourquoi nous demande-t-on une **confiance aveugle** en un système informatique dont l'intégrité est vaguement contrôlée par une poignée de techniciens mal identifiés ?

La confiance envers les hommes politiques ou leur possibilité d'action est déjà entamée. Il serait dangereux d'y ajouter une méfiance vis à vis de l'honnêteté des élections.

Voici maintenant quelques questions précises :

Comment rendre au citoyen le contrôle de l'élection, comme le commandent les principes de la démocratie représentative[56] ?

Quel mécanisme garantit le contenu des ordinateurs de vote, notamment l'authenticité de leur logiciel ? Nous n'en voyons aucun de sérieux, et nous estimons qu'il n'y a pas de solution réaliste.

Si une élection est contestée, qui apparaîtra responsable de l'incertitude créée par le vote électronique[57] ? A qui sera reprochée une insuffisance de contrôle ?

Quelle est l'explication du marketing invraisemblable pratiqué par Nedap/France-Élection[58], qui cherche à faire croire que ses ordinateurs sont de «simples objets électroniques» ? Aucun informaticien ne peut prendre au sérieux de telles affirmations.

---

52 Afin de ne pas insulter l'avenir, les pétitions, telles celle de David Dill, ou celle de "the free e-democracy project", utilisent l'expression "trace d'audit vérifiée par l'électeur". Elles précisent ensuite qu'en l'état actuel des connaissances, seul le papier permet de réaliser cette trace d'audit.

53 Sur notre site : le bulletin papier vérifié par l'électeur (VVPB/VVAT), détails de ce concept, difficultés de mise en oeuvre, et réalisations (bâclées) à l'étranger.

54 "L'argent public ne doit payer qu'une fois", comme le dit l'ADULLACT.

55 Cf Wikipedia (en anglais) : "Security through obscurity".Un usage raisonnable du secret est possible, en s'inspirant de la cryptographie : les logiciels et méthodes de calculs (algorithmes) sont publics, seule la clef étant secrète. Dans le cas du vote électronique, voir le rapport CEV, app. 2B, page145, Appendix B.

56 Selon la CNIL, "le recours à des techniques informatiques sophistiquées ne doit pas conduire à faire échapper les systèmes de vote au contrôle démocratique des membres du bureau de vote, des scrutateurs et des électeurs au profit de techniciens informatiques.". Malheureusement, la transition avec le paragraphe suivant est "schizophrénique" Rapport 2003, page 94.

57 "Aucun des systèmes de vote connus de la CNIL ne prévoient de produire des éléments de preuve en cas de contentieux électoral. Ces éléments de preuve s'entendent sur le fonctionnement du système de vote lui-même lors du déroulement du scrutin, de manière à démontrer de façon convaincante qu'il n'a pas donné lieu à un fonctionnement anormal, que celui-ci soit involontaire ou délibéré." Rapport CNIL 2003, page 93.

58 Cf note n°14.

Pourquoi une telle opacité entoure-t-elle le vote électronique, allant même jusqu'aux rapports d'agrément ?

La CNIL a recommandé une “évaluation globale des dispositifs de vote électronique”, quand sera-t-elle réalisée ? Faut-il aller plus loin, et suivre l'exemple de l'Irlande et des Pays-Bas, en créant une commission officielle pour enquêter sur le vote électronique ?

www.**ordinateurs-de-vote**.org

Texte de Pierre Muller, contact@recul-democratique.org,
tél 09 53 18 27 54 (tarification locale) / 06 63 72 63 56

Ordinateurs Nedap/France-Élection : la vérification de checksums est une duperie

L'explication qui suit est un peu technique. Il est tout à fait naturel que vous ne la compreniez pas. Nous vous invitons alors à la soumettre à quelqu'un de votre entourage ayant quelques bases en informatique. ***Que vous ne compreniez pas est néanmoins significatif.*** *Si vous étiez assesseur, vous auriez l'illusion d'effectuer un contrôle de l'ordinateur, mais la présence de technologie vous empêcherait d'exercer votre sens critique, et de comprendre que ce contrôle est inopérant.*

Lors de la procédure d'agrément, un seul ordinateur (ou tout au plus quelques uns), sont examinés par l’organisme d’inspection. L'agrément est accordé sur un modèle d'ordinateur, et non pas pour chaque exemplaire fabriqué de cet ordinateur. Il est donc crucial de garantir que tous les ordinateurs présents dans les bureaux de vote soient identiques à celui examiné. Un point essentiel est le logiciel intégré, car l'essentiel de l'intelligence de l'ordinateur de vote y réside.

France-Élection, importateur des ordinateurs Nedap, prétend contrôler l'authenticité de ce logiciel au moyen de la vérification des checksums. De quoi s'agit-il ? L'ordinateur de vote sait calculer un nombre appelé checksum (en français : somme de contrôle) à partir de tous les 0 et 1 qui constituent son logiciel intégré. Si le moindre de ces 0 ou 1 est modifié, ce checksum va changer de valeur. En pratique, deux checksums sont calculés, chacun concernant la moitié de la mémoire. Leur valeur est indiquée dans le manuel d'utilisation de l'ordinateur. Le matin de l'élection, les assesseurs doivent donc demander à l'ordinateur d'imprimer ces checksums et vérifier qu'ils soient identiques à ce qu'indique le manuel.

Cette procédure est recommandée et considérée comme efficace par le rapport du PTB (Physikalisch-Technische Bundesanstalt), organisme en charge de certifier le logiciel intégré. A l'exigence[59] *"Dans le cas d'une machine à microprocesseur, toute altération du logiciel intégré par une personne non autorisée sera détectée."*, le PTB répond que l'exigence est satisfaite, et se justifie ainsi:

"Les numéros de version des programmes et les checksums du logiciel intégré, pour la carte principale de contrôle, la carte de connexion (communication), et les cinq cartes d'affichage peuvent être affichés, et imprimés, par l'ordinateur de vote.

Cela permet au personnel électoral de comparer ces numéros de version des programmes et ces checksums avec les valeurs indiquées par le fabricant dans la documentation (manuel d'utilisateur), ou par exemple inscrits sur un certificat agréé."

Qu'est-ce qui ne va pas ? C'est déjà se tromper de technologie[60], mais finalement, cela n'a guère d'importance : ***le principe même de cette vérification est inepte***, quelle que soit la technologie employée. En effet, on demande d'imprimer ce checksum au logiciel que l'on cherche à contrôler. L'alternative se présente ainsi : soit il est authentique, et il va réellement le calculer et le résultat sera conforme, sauf défaillance de l'électronique ; soit il a été modifié frauduleusement, et il se gardera de

---

59 "Type testing of a voting machine for elections/referenda in Ireland...", page 7, exigence (4).

60 Un checksum a pour vocation de détecter des modifications ***accidentelles*** : par exemple si l'un des 0 ou 1 s'est modifié à cause d'une défaillance physique de la puce électronique qui le stocke. Par contre, cela ne protège pas des modifications ***intentionnelles***: à cet effet, on utilisera la technique du hash cryptographique.

faire le moindre calcul, et se contentera d'imprimer la valeur indiquée dans le manuel d'utilisateur. L'infinie flexibilité d'un logiciel fait que cela ne pose aucune difficulté de réalisation.

Dans le cadre d'une expertise judiciaire d'un ordinateur, on ne l'allume surtout pas. On le démonte pour en extraire ses mémoires (en général son disque dur), et on les place dans un autre ordinateur que l'on considère comme sûr.

Faire confiance à cette vérification de checksum est comme d'arrêter un inconnu dans la rue, de lui demander si il est honnête, et en cas de réponse affirmative, de le charger de faire un retrait d'argent en lui confiant notre carte bleue.

L'ineptie de cette vérification de checksum a été pointée dans le rapport[61] de la Commission on Electronic Voting, commission indépendante qui a déconseillé l'utilisation des ordinateurs Nedap en Irlande.

Par quel bout que l'on prenne cette procédure de vérification de checksum, on n'en comprend pas la mise en oeuvre. En effet, si l'objectif se réduisait à vérifier le bon fonctionnement de l'électronique, une procédure bien plus simple suffirait : si tout va bien, l'ordinateur démarre sans rien dire, sinon il s'arrête en affichant un message d'erreur. Tous les PC du monde vérifient ainsi leur mémoire lorsqu'on les allume[62], sans pour autant vous demander d'aller consulter leur manuel d'utilisation. L'ordinateur Nedap utilise d'ailleurs à cet usage un troisième checksum interne.

La difficulté de contrôle de l'authenticité du logiciel intégré est générale à tous les ordinateurs de vote. Les ordinateurs concurrents Indra et ES&S iVotronic ne font pas mieux. Ils ne tentent même pas de réaliser cette vérification du logiciel intégré. On peut toutefois leur reconnaître le mérite de la franchise.

Depuis peu, France-Élection a adapté sa communication. L'accent est mis sur les scellés (des étiquettes métallisées posées par eux-mêmes), mais la vérification des checksums reste considérée comme utile.

Le code source, définition

L'essentiel de l'intelligence d'un système informatique est dans son logiciel (en anglais : "software"). Celui-ci existe sous deux formes :

- le "code source" : écrit et lisible par des humains, plus précisément une peuplade appelée programmeurs ou développeurs. C'est la description méthodique, et dans les moindres détails, de tout ce que fait le logiciel. Cette description est tapée comme vous taperiez une lettre, mais au lieu du français, dans un langage informatique. Il en existe des centaines, les plus connus ont pour nom : C, C++, Pascal, Basic, Java... Ces langages ont comme particularité de ne permettre aucune ambiguïté, contrairement aux langages naturels où un mot peut avoir plusieurs sens.
- le "code binaire" ou "exécutable" formé de 0 et de 1, donc uniquement exploitable par l'ordinateur. Il est produit automatiquement à partir du "code source" au moyen d'une moulinette appelée compilateur. Il va faire s'animer l'ordinateur, au départ simple assemblage électronique inerte (en anglais : "hardware", traduit par "matériel").

A l'exception notable des Logiciels Libres, vous n'achetez qu'un droit d'utilisation de l'exécutable. Le code source reste secret et propriété de son concepteur. Sans lui, vous ne pourrez qu'observer le comportement apparent de l'exécutable. Des fonctionnalités cachées (oeuf de Pâques, cheat codes, backdoors...) ne se révéleront pas si on ne connaît pas l'astuce pour les déclencher.

61 «Le programme intégré à l'ordinateur de vote pourrait être modifié pour altérer les votes. Le programme a un checksum, qui le protège contre des modifications accidentelles, mais qui ne protège pas contre des manipulations délibérées.»

62 Pour être précis, il s'agit de vérifier la mémoire vive (RAM), et non pas la mémoire morte (ROM ou EPROM).